PEER TO PEER FILE SHARING

1. Based on my training and experience I know the following regarding Peer to Peer file sharing networks, and Peer to Peer client software programs.

   a. One common use on the Internet is peer to peer (hereinafter referred to as "P2P") file sharing. P2P file sharing is a method of communication available to Internet users through the use of special software programs. P2P file sharing programs allow groups of computers using the same file sharing network and protocols to transfer digital files from one computer system to another while connected to a network, usually on the Internet. There are multiple types of P2P file sharing networks on the Internet. To connect to a particular P2P file sharing network, a user first obtains a P2P client software program for a particular P2P file sharing network, which can be downloaded from the Internet. A particular P2P file sharing network may have many different P2P client software programs that allow access to that particular P2P file sharing network. Additionally, a particular P2P client software program may be able to access multiple P2P file sharing networks. These P2P client software programs share common protocols for network access and file sharing. The user interface, features, and configurations may vary between clients and versions of the same client.

   b. In general, P2P client software allows the user to set up file(s) on a computer to be shared on a P2P file sharing network with other users running compatible P2P client software. A user can also obtain files by opening the P2P client software on the user's computer and conducting a search for files that are of interest and currently being shared on a P2P file sharing network.

   c. Some P2P file sharing networks are designed to allow users to download files and frequently provide enhanced capabilities to reward the sharing of files by providing reduced wait periods, higher user ratings, or other benefits. In some instances, users are not allowed to download files if they are not sharing files. Typically, settings within these programs control sharing thresholds.

   d. Typically, during a default installation of a P2P client software program, settings are established which configure the host computer to share files. Depending upon the P2P client software used, a user may have the ability to reconfigure some of those settings during installation or after the installation has been completed.

   e. Typically, a setting establishes the location of one or more directories or folders whose contents (digital files) are made available for distribution to other P2P clients. In some clients, individual files can also be shared.

   f. Typically, a setting controls whether or not files are made available for distribution to other P2P clients.

g. Typically, a setting controls whether or not users will be able to share portions of a file while they are in the process of downloading the entire file. This feature increases the efficiency of the network by putting more copies of file segments on the network for distribution.

h. Typically, files being shared by P2P clients are processed by the client software. As part of this processing, a hashed algorithm value is computed for each file and/or piece of a file being shared (dependent on the P2P file sharing network), which uniquely identifies it on the network. A file (or piece of a file) processed by this hash algorithm operation results in the creation of an associated hash value often referred to as a digital signature. By using a hash algorithm to uniquely identify files on a P2P network, it improves the network efficiency. Because of this, typically, users may receive a selected file from numerous sources by accepting segments of the same file from multiple clients and then reassembling the complete file on the local computer. This is referred to as multiple source downloads. The client program succeeds in reassembling the file from different sources only if all the segments came from exact copies of the same file. P2P file sharing networks use hash values to ensure exact copies of the same file are used during this process.

i. P2P file sharing networks, including the BitTorrent network, are frequently used to trade digital files of child pornography. These files include both image and movie files.

BITTORRENT NETWORKS

2. Based on my training and experience I know the following regarding the BitTorrent Peer to Peer file sharing network.

a. The BitTorrent network is a very popular and publicly available peer to peer file sharing network. Most computers that are part of this network are referred to as “peers”. The terms “peers” and “clients” can be used interchangeably when referring to the BitTorrent network. A peer can simultaneously provide files to some peers while downloading files from other peers.

b. The BitTorrent network can be accessed by computers running many different client programs, some of which include the BitTorrent client program, uTorrent client program, and Vuze client program. These client programs are publicly available and free P2P client software programs that can be downloaded from the Internet. There are also BitTorrent client programs that are not free. These BitTorrent client programs share common protocols for network access and file sharing. The user interface, features, and configuration may vary between clients and versions of the same client.

c. During the installation of typical BitTorrent network client programs, various settings are established which configure the host computer to share files.

Generally, when installing onto a computer the user has pop up notifications that alert the user that the user will be sharing files. Users cannot prevent sharing while a file is being actively downloaded. Depending upon the BitTorrent client used, a user may have the ability to reconfigure some of those settings during installation or after the installation has been completed. Typically, a setting establishes the location of one or more directories or folders whose contents (files) are made available to other BitTorrent network users to download.

d. In order to share a file or a set of files on the BitTorrent network, a "Torrent" file needs to be created by the user that initially wants to share the file or set of files. A "Torrent" is typically a small file that describes the file(s) that are being shared, which may include information on how to locate the file(s) on the BitTorrent network. A typical BitTorrent client will have the ability to create a "Torrent" file. It is important to note that the "Torrent" file does not contain the actual file(s) being shared, but information about the file(s) described in the "Torrent", such as the name(s) of the file(s) being referenced in the "Torrent" and the "info hash" of the "Torrent". The "info hash" is a SHA-1 hash value of the set of data describing the file(s) referenced in the "Torrent", which include the SHA-1 hash value of each file piece, the file size, and the file name(s). The "info hash" of each "Torrent" uniquely identifies the "Torrent" file on the BitTorrent network. The "Torrent" file may also contain information on how to locate file(s) referenced in the "Torrent" by identifying "Trackers". "Trackers" are computers on the BitTorrent network that collate information about the peers/clients that have recently reported they are sharing the file(s) referenced in the "Torrent" file. A "Tracker" is only a pointer to peers/clients on the network who may be sharing part or all of the file(s) referenced in the "Torrent". It is important to note that the "Trackers" do not actually have the file(s) and are used to facilitate the finding of other peers/clients that have the entire file(s) or at least a portion of the file(s) available for sharing. It should also be noted that the use of "Tracker(s)" on the BitTorrent network are not always necessary to locate peers/clients that have file(s) being shared from a particular "Torrent" file. There are many publicly available servers on the Internet that provide BitTorrent tracker services.

e. Once a torrent is created, in order to share the file(s) referenced in the "Torrent" file, a user typically makes the "Torrent" available to other users, such as via websites on the Internet.

f. In order to locate "Torrent" files of interest, a typical user will use keyword searches within the BitTorrent network client itself or on websites hosting "Torrents". Once a "Torrent" file is located that meets the keyword search criteria, the user will download the "Torrent" file to their computer. Alternatively, a user can also search for and locate "magnet links", which is a link that enables the BitTorrent network client program itself to download the "Torrent" to the computer. In either case, a "Torrent" file is downloaded to the user's computer. The BitTorrent network client will then process that "Torrent" file in order to find "Trackers" or utilize other means that will help facilitate finding other peers/clients

on the network that have all or part of the file(s) referenced in the “Torrent” file. It is again important to note that the actual file(s) referenced in the “Torrent” are actually obtained directly from other peers/clients on the BitTorrent network and not the “Trackers” themselves. Typically, the “Trackers” on the network return information about remote peers/clients that have recently reported they have the same file(s) available for sharing (based on SHA-1 “info hash” value comparison), or parts of the same file(s), referenced in the “Torrent”, to include the remote peers/clients Internet Protocol (IP) addresses.

g. For example, a person interested in obtaining child pornographic images on the BitTorrent network would open the BitTorrent client application on his/her computer and conduct a keyword search for files using a term such as "preteen sex." The results of the torrent search are typically returned to the user's computer by displaying them on the torrent hosting website. The hosting website will typically display information about the torrent, which can include the name of the torrent file, the name of the file(s) referenced in the torrent file, the file(s) size, and the “info hash” SHA-1 value of the torrent file. The user then selects a torrent of interest to download to their computer. Typically, the BitTorrent client program will then process the torrent file. The user selects from the results displayed the file(s) they want to download that were referenced in the torrent file. Utilizing trackers and other BitTorrent network protocols (such as Distributed Hash Tables, Peer Exchange, and Local Peer Discovery), peers/clients are located that have recently reported they have the file(s) or parts of the file(s) referenced in the torrent file available for sharing. The file(s) is then downloaded directly from the computer(s) sharing the file. Typically, once the BitTorrent network client has downloaded part of a file(s), it may immediately begin sharing the file with other users on the network. The BitTorrent network client program succeeds in reassembling the file(s) from different sources only if it receives “pieces” with the exact SHA-1 piece hash described in the torrent file. During the download process, a typical BitTorrent client program displays the Internet Protocol address of the peers/clients that appear to be sharing part or all of the file(s) referenced in the torrent file or other methods utilized by the BitTorrent network protocols. The downloaded file is then stored in the area previously designated by the user and/or the client program. The downloaded file(s), including the torrent file, will remain until moved or deleted.

h. Typically, as described above, one method for an investigator to search the BitTorrent network for users possessing and/or disseminating child pornography files is to type in search terms, based on their training and experience, that would return a torrent filename indicative of child pornography. The investigator would then download the file(s) referenced within the torrent file and determine if the file(s) indeed contained child pornography. If so, the investigator can document the “info hash” SHA-1 hash value of this torrent file, to be compared with future identical torrent files observed on the BitTorrent network. Although transparent to the typical user, when searches are conducted, additional results are received from the trackers on other peers who recently reported to the network as having

that file(s) in whole or in part, which may include the IP addresses of those peers/clients. This information can be documented by investigators and compared to those "info hash" SHA-1 hash values the investigator has obtained in the past and believes to be child pornography. This allows for the detection and investigation of computers involved in possessing, receiving, and/or distributing files of previously identified child pornography. Therefore, without even downloading the file, the investigator can compare the "info hash" SHA-1 hash value and determine with mathematical certainty that a file(s) seen on the network is an identical copy of a child pornography file(s) they had seen before.

i. The returned list of IP addresses can include computers that are likely to be within the investigator's jurisdiction. The ability to identify the approximate location of these IP addresses is provided by IP geographic mapping services, which are publicly available and also used for marketing and fraud detection. At this point in the investigative process, an association between a known torrent file (based upon on the "info hash" SHA-1 hash value comparison) and a computer having a specific IP address (likely to be located within a specific region) can be established.

j. Once a client user is identified as recently having a file(s) believed to be child pornography, in whole or in part, the investigator can then query that client user directly to confirm the client user has that file(s), in whole or in part, and/or download that file directly from the client user exclusively, otherwise known as a single source download. Depending upon several factors, including configuration and available resources, it might not be possible to do either. The process of sharing files on the BitTorrent network involves peers allowing other peers to copy a file(s) or portions of a file(s). This sharing process does not remove the file(s) from the computer sharing the file. This process places a copy of the file on the computer which downloaded it.

k. If an investigator either received an affirmative response from a remote peer that they possess a digital file, or the investigator received a digital file, in whole or in part, that is believed to contain child pornography, from a remote peer at a specific IP address, the investigator can conclude that a computer, likely to be in this jurisdiction, is running a BitTorrent network P2P client and is currently possessing, receiving, and/or distributing specific and known visual depictions of child pornography.

l. Law Enforcement has created BitTorrent network client programs that obtain information from "Trackers" about peers/clients recently reporting that they are involved in sharing digital files of known actual child pornography (based on the "info hash" SHA-1 hash value), which then allows the downloading of a file from a single IP address (as opposed to obtaining the file from multiple peers/clients on the network). This procedure allows for the detection and investigation of those computers involved in sharing digital files of known actual child pornography on the BitTorrent network.

m. During the query and/or downloading process from a remote BitTorrent network client, certain information may be exchanged between the investigator's client and the remote client they are querying and/or downloading a file from. Such as 1) the remote client's IP address; 2) a confirmation from the remote client that they have pieces of the file(s) being requested, in whole or in part, and that the pieces of the file(s) are being reported as shared from the remote client program; and 3) the remote client program and version. This information may remain on the remote client's computer system for long periods of time. The investigator has the ability to log this information. A search can later be conducted on a seized computer system(s) for this information, which may provide further evidence that the investigator's client communicated with the remote client.

3. An analogy to this investigative methodology would be receiving information from an informant or an anonymous source that a particular residence was selling illegal narcotics. An undercover investigator could independently confirm this information by knocking on the door of the residence and asking if they had said illegal narcotics. If so, the undercover investigator would then ask for and receive the said illegal narcotics without entering the residence, which would be similar to asking for and receiving an illegal child pornography file from a P2P peer/client.

4. The investigation of peer-to-peer file sharing networks is a cooperative effort of law enforcement agencies around the country. Many of these agencies are associated with the ICAC Task Force Program. P2P investigative methodology has led to the issuance and execution of search warrants around the country resulting in the arrest and conviction of numerous offenders possessing and/or distributing child pornography, some of which were also involved in the sexual exploitation of actual child victims. The Wyoming ICAC utilizes Roundup tools that have been tailored for law enforcement as mentioned above to ensure it focuses on user withing the boundaries of Wyoming and conducts only single source downloads from those users.

Gary Seder

Gary Seder, Agent
Wyoming Division of Criminal Investigation